PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of	Docket No: Q64734
Francis PINAULT, et al.	
Appln. No.: 09/873,357	Group Art Unit: 2134
Confirmation No.: 5168	Examiner: Piotr POLTORAK
Filed: June 5, 2001	

For: METHOD OF PROVIDING ACCESS CONTROL FOR AND/OR VIS-A-VIS USERS ACCESSING THE INTERNET FROM TERMINALS VIA A PRIVATE ACCESS NODE, AND ARRANGEMENTS FOR PUTTING THIS KIND OF METHOD INTO PRACTICE

SUBMISSION OF APPEAL BRIEF

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The USPTO is directed and authorized to charge the statutory fee of $510.00 and all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880.

Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

Theodore C. Shih
Registration No. 60,645

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: May 5, 2008

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of	Docket No: Q64734
Francis PINAULT, et al.	
Appln. No.: 09/873,357	Group Art Unit: 2134
Confirmation No.: 5168	Examiner: Piotr POLTORAK
Filed: June 5, 2001	

For: METHOD OF PROVIDING ACCESS CONTROL FOR AND/OR VIS-A-VIS USERS ACCESSING THE INTERNET FROM TERMINALS VIA A PRIVATE ACCESS NODE, AND ARRANGEMENTS FOR PUTTING THIS KIND OF METHOD INTO PRACTICE

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 41.37, Appellant submits the following:

Table of Contents

I. REAL PARTY IN INTEREST

The real party in interest is ALCATEL, by virtue of an assignment executed by Francis PINAULT and Alain GUIRAUTON (Appellants, hereafter), on May 15, 2001, and recorded by the Assignment branch of the U.S. Patent and Trademark Office on June 5, 2001 (at Reel 011885, Frame 0501).

II. RELATED APPEALS AND INTERFERENCES

To the knowledge and belief of Appellants, the Assignee, and the undersigned, there are no other appeals or interferences before the Board of Appeals and Interferences that will directly affect or be affected by the Board's decision in the instant Appeal.

III. STATUS OF CLAIMS

The Application was originally filed with claims 1-10, and claims 1, 2, and 4-13 are the currently pending claims.

Claims 1, 2, 4, and 8-13 stand rejected under 35 U.S.C. § 102(a) as anticipated by or, in the alternative, rejected under 35 U.S.C. § 103(a) as being unpatentable over Toga (U.S. 6,041,355); claims 5-7 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Toga in view of Fritch (U.S. 6,105,132) in view of Cotten (U.S. 6,330,590), claim 13 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Toga in view of Hitson (U.S. Pub. No. 2002/0010759).

The rejections of claims 1, 2, and 4-13 are being appealed.

IV. STATUS OF AMENDMENTS

As of the advisory Action dated January 7, 2008, the Examiner has entered the proposed amendments and no outstanding amendments to the claims are currently pending. Thus the claims stand as presented prior to the Final Office Action dated October 2, 2007.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The instant application is directed toward an apparatus for providing access control for user terminals connected to a private network, and a method of operation thereof. According to claim 1, disclosed is a method of providing access control for user terminals connected to a private network, wherein said terminals access a computer network enabling exchange of information via a private access node to which said terminals are connected and an access server, the method comprising:

temporarily storing a multimedia data stream received from said computer network and addressed to a user terminal[1] of said user terminals connected to said private network in response to an access request from said user terminal in order to perform filtering based on data content of said multimedia data stream, said filtering, authorizing or blocking transmission of said multimedia data stream to said terminal as a function of particular criteria provided from said private network and applied to the multimedia data stream received at said private access node[2], and

analyzing a signature included in said multimedia data stream for the purpose of said filtering[3].

---

[1] See FIG. 2, and page 7, lines 25-35.

[2] See page 8, lines 1-9.

[3] See page 9, lines 9-16.

According to claim 10, disclosed is an apparatus for providing access control for user terminals connected to a private network, wherein said terminals access a computer network enabling exchange of information via a private access node to which said terminals are connected and a service provider, organized to authorize or block transmission of said data stream to said terminals, the apparatus comprising:

a storage unit[4] for temporarily storing a multimedia data stream[5] received from said computer network[6] and addressed to a user terminal[7] of said user terminals connected to said private network in response to an access request from said user terminal,

a control logic unit[8] for filtering said multimedia data stream stored in said storage unit, said filtering authorizing or blocking transmission of said multimedia data stream to said terminal as a function of particular criteria provided from said private network and applied to data content which comprises said multimedia data stream received at said private access node, and analyzing a signature[9] included in said multimedia data stream for the purpose of said filtering.

---

[4] See FIG. 2, element 7.

[5] See page 7, lines 31-34.

[6] See FIG. 1, element 3.

[7] See FIG. 1, element 1.

[8] See FIG. 2, element 6.

[9] See page 10, lines 13-14.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1, 2, 4, and 8-13 stand rejected under 35 U.S.C. § 102(a) as anticipated by or, in the alternative, rejected under 35 U.S.C. § 103(a) as being unpatentable over Toga (U.S. 6,041,355).

2. Claims 5-7 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Toga in view of Fritch (U.S. 6,105,132)[10] in view of Cotten (U.S. 6,330,590).

3. Claim 13 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Toga in view of Hitson (U.S. Pub. No. 2002/0010759).

[10] Applicant notes that Fritch is never discussed in the body of the rejection. It further appears that the citation is a typo and that the Examiner only intended to reject the claims over Toga in view of Cotten.

VII. ARGUMENT

1. Claims 1, 2, 4, and 8-13 stand rejected under 35 U.S.C. § 102(a) as anticipated by or, in the alternative, rejected under 35 U.S.C. § 103(a) as being unpatentable over Toga.

Claim 1

Appellants respectfully submit that independent claim 1 is not anticipated by or unpatentable over Toga.

Claim 1 recites:

> A method of providing access control for user terminals connected to a private network, wherein said terminals access a computer network enabling exchange of information via a private access node to which said terminals are connected and an access server, the method comprising:
>
> temporarily storing a multimedia data stream received from said computer network and addressed to a user terminal of said user terminals connected to said private network in response to an access request from said user terminal in order to perform filtering based on data content of said multimedia data stream, said filtering, authorizing or blocking transmission of said multimedia data stream to said terminal as a function of particular criteria provided from said private network and applied to the multimedia data stream received at said private access node, and
>
> analyzing a signature included in said multimedia data stream for the purpose of said filtering.

Toga discloses "a method of controlling the transfer of data between a first and second computer network comprises parsing content description language received from the first computer network by the second computer network to determine current tag information within the content description language". See the abstract. Toga, however, fails to disclose "analyzing ***a signature*** included in said multimedia data stream for the purpose of said filtering" as recited in claim 1. Instead, Toga, focuses on tags, which are used for displaying the data in an appropriate manner

by a browser. In Toga, tags may convey other information about the content of data and be used by the proxy to determine whether to allow subsequent data transfer. See col. 3, lines 33-45.

In the Advisory Action, the Examiner argues:

> Applicant's focuses on a term "signature" and argues that Toga teaches tag information which is not the same as signature. Thus, applicant argues, Toga does not teach "analyzing a signature included in said multimedia data stream". In order to articulate support this assertion, applicant argues that tag disclosed by Toga are not a signature as defined in the art.
>
> The examiner respectfully disagrees. Signature may mean different things in different arts. For example, in the art of computer security (i.e. utilizing cryptography) the signature has a very special meaning and does not equate to restriction, as applicant suggest. Although applicant's application could be considered to address computer security (filtering data stream) nowhere in the specification applicant suggest that the signature is the same as cryptographic signature. In fact, there is no clear definition offered in the specification. Thus, the examiner's broadest interpretation of the term does not violate the reasonable interpretation of the term[11].

Based on the above comments, the Examiner did not respond to the crux of the argument presented in the Response filed December 28, 2007. Specifically, the Examiner fails to rebut the argument that the Toga reference does not teach, "analyzing a ***signature*** included in said multimedia data stream for the purpose of said filtering" as recited in claim 1. Specifically, the "tag information" in Toga refers to displaying the data (by indicating tags within content description language), financial tags, resource constraints tags, and content restriction tags. While, in the present invention, signatures are used for the purposes of allowing or restricting multimedia data stream regardless of the "tag information" definitions of Toga.

---

[11] *See* Advisory Action mailed January 7, 2008.

Furthermore, Applicants' specification clearly states an exemplary embodiment of the "signature" where the "signature" can indicate the existence of restrictions on the use of the data that it accompanies and in particular to SDMI (secure digital music initiative) signatures accompanying data constituting certain multimedia files (see page 10, lines 13-16).

For the above reasons, Applicant submits that claim 1 is patentable over the applied art. Claims 2, 4, 8-9, 11, 12, and 13 are patentable at least by virtue of its dependency on claim 1.

Claim 10

Appellants respectfully submit that independent claim 10 is not anticipated by or unpatentable over Toga.

Claim 10 recites, in part:

> a control logic unit for filtering said multimedia data stream stored in said storage unit, said filtering authorizing or blocking transmission of said multimedia data stream to said terminal as a function of particular criteria provided from said private network and applied to data content which comprises said multimedia data stream received at said private access node, and ***analyzing a signature*** included in said multimedia data stream for the purpose of said filtering.

Toga discloses "a method of controlling the transfer of data between a first and second computer network comprises parsing content description language received from the first computer network by the second computer network to determine current tag information within the content description language". See the abstract. Toga, however, fails to disclose "analyzing ***a signature*** included in said multimedia data stream for the purpose of said filtering" as recited in claim 10. Instead, Toga, focuses on tags, which are used for displaying the data in an appropriate manner

by a browser. In Toga, tags may convey other information about the content of data and be used by the proxy to determine whether to allow subsequent data transfer. See col. 3, lines 33-45.

In the Advisory Action, the Examiner argues:

> Applicant's focuses on a term "signature" and argues that Toga teaches tag information which is not the same as signature. Thus, applicant argues, Toga does not teach "analyzing a signature included in said multimedia data stream". In order to articulate support this assertion, applicant argues that tag disclosed by Toga are not a signature as defined in the art.
>
> The examiner respectfully disagrees. Signature may mean different things in different arts. For example, in the art of computer security (i.e. utilizing cryptography) the signature has a very special meaning and does not equate to restriction, as applicant suggest. Although applicant's application could be considered to address computer security (filtering data stream) nowhere in the specification applicant suggest that the signature is the same as cryptographic signature. In fact, there is no clear definition offered in the specification. Thus, the examiner's broadest interpretation of the term does not violate the reasonable interpretation of the term[12].

Based on the above comments, the Examiner did not respond to the crux of the argument presented in the Response filed December 28, 2007. Specifically, the Examiner fails to rebut the argument that the Toga reference does not teach, "analyzing a ***signature*** included in said multimedia data stream for the purpose of said filtering" as recited in claim 10. Specifically, the "tag information" in Toga refers to displaying the data (by indicating tags within content description language), financial tags, resource constraints tags, and content restriction tags. While, in the present invention, signatures are used for the purposes of allowing or restricting multimedia data stream regardless of the "tag information" definitions of Toga.

---

[12] *See* Advisory Action mailed January 7, 2008.

Furthermore, Applicants' specification clearly states an exemplary embodiment of the "signature" where the "signature" can indicate the existence of restrictions on the use of the data that it accompanies and in particular to SDMI (secure digital music initiative) signatures accompanying data constituting certain multimedia files (see page 10, lines 13-16).

2. Claims 5-7 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Toga in view of Fritch in view of Cotton.

Appellants respectfully submit that claims 5-7 are not anticipated by or unpatentable over Toga in view of Fritch in view of Cotton.

The Examiner admits that "Toga in view of Fritch do [not] explicitly teach retaining non-conformance data to enable interruption of a subsequently received data stream," but asserts that "Cotton teaches counting, for control purposes, the number of times that data of a particular content is received and retaining non-conformance data to enable interruption of a subsequently received data stream", citing in support col. 3, line 46 to col. 4, line 52. Further, the Examiner concludes that "it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to retain non-conformance data to enable interruption of a subsequently received data stream as taught by Cotton. One of ordinary skill in the art would have been motivated to perform such a modification in order to filter not only non-permitted but also unwanted data."

Cotton relates to method and system for detecting bulk email. The bulk e-mail is detected by monitoring live e-mails flow stream…after detection, a numerical signature identification code is established. See col. 2, line 17-34. Therefore, Cotton does not cure

the deficient teachings of Toga. For example, Cotton does not teach "analyzing a signature included in said multimedia data stream for the purpose of said filtering." Emphasis added.

Moreover, Cotton only teaches to store in a register the signature which was calculated in the detecting step as discussed above. Id, see also, col. 3, lines 51-55, and col. 4, line 19-24. This teaching is not analogous to that "said multimedia data stream stores in the determination of conformance", as recited in claim 5 or "data for which non-conformance has been detected in said multimedia data stream is retained to enable interruption of subsequently received multimedia data stream", as recited in claim 6. Therefore, for at least these reasons, Applicant submits that the claims are not obvious in view of the combination.

3. Claim 13 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Toga in view of Hitson.

Claim 13 is patentable at least by virtue of their dependency from claim 1, as Hitson fails to cure the deficient disclosure of Toga.

Conclusion

Applicant herewith petitions the Director of the USPTO to extend the time for reply to the above-identified Office Action for an appropriate length of time if necessary. Unless a check is attached, any fee due under 37 U.S.C. § 1.17(a) is being paid via the USPTO Electronic Filing System (EFS).

Unless a check is submitted herewith for the fee required under 37 C.F.R. §41.37(a) and 1.17(c), please charge said fee to Deposit Account No. 19-4880.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

Theodore C. Shih
Registration No. 60,645

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860
WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: May 5, 2008

CLAIMS APPENDIX

CLAIMS 1, 2, and 4-13 ON APPEAL:

1. A method of providing access control for user terminals connected to a private network, wherein said terminals access a computer network enabling exchange of information via a private access node to which said terminals are connected and an access server, the method comprising:

temporarily storing a multimedia data stream received from said computer network and addressed to a user terminal of said user terminals connected to said private network in response to an access request from said user terminal in order to perform filtering based on data content of said multimedia data stream, said filtering, authorizing or blocking transmission of said multimedia data stream to said terminal as a function of particular criteria provided from said private network and applied to the multimedia data stream received at said private access node, and

analyzing a signature included in said multimedia data stream for the purpose of said filtering.

2. The method claimed in claim 1, wherein said multimedia data stream received from said computer network is stored temporarily before it is transmitted to said user terminal depending on results of said filtering.

3. (Cancelled)

4. The method claimed in claim 1, wherein transfer of said multimedia data stream received from said computer network to a user terminal is temporarily delayed pending determination of conformance of said multimedia data stream which has been received with particular standards and then transmitted to said terminal if conformance is found.

5. The method claimed in claim 4, wherein temporarily delayed data, which comprises said multimedia data stream stored in the determination of conformance, is retained to enable a further check in the event of non-conformance, either in respect of data received on detection of non-conformance, in which case the multimedia data stream is interrupted, or in respect of all data of the multimedia data stream received, without said multimedia data stream being interrupted.

6. The method claimed in claim 4, wherein data for which non-conformance has been detected in said multimedia data stream is retained to enable interruption of a subsequently received multimedia data stream before complete analysis of said subsequently received multimedia data stream if said data is detected again in said subsequently received multimedia data stream.

7. The method claimed in claim 1, further comprising counting, for control purposes, the number of times that data of a particular content is received, if said content is found in said multimedia data stream which is temporarily stored, after it has been received from said computer network in at least one data stream addressed to a particular terminal.

8. The method claimed in claim 2, further comprising performing signature analysis for at least temporarily blocking transmission of said multimedia data stream received from said network to a user terminal if said multimedia data stream incorporates a signature characteristic of restricted signaling rights.

9. The method claimed in claim 2, further comprising performing an identifier search analysis on said multimedia data stream addressed to a user terminal to authorize transmission of said multimedia data stream to said terminal if an identifier is found in the multimedia data stream addressed to said terminal.

10. An apparatus for providing access control for user terminals connected to a private network, wherein said terminals access a computer network enabling exchange of information via a private access node to which said terminals are connected and a service provider, organized to authorize or block transmission of said data stream to said terminals, the apparatus comprising:

a storage unit for temporarily storing a multimedia data stream received from said computer network and addressed to a user terminal of said user terminals connected to said private network in response to an access request from said user terminal,

a control logic unit for filtering said multimedia data stream stored in said storage unit, said filtering authorizing or blocking transmission of said multimedia data stream to said terminal as a function of particular criteria provided from said private network and applied to data content which comprises said multimedia data stream received at said private access node, and analyzing a signature included in said multimedia data stream for the purpose of said filtering.

11. The method of providing access control for user terminals connected to a private network according to claim 1, wherein performing filtering based on data content of said multimedia data stream comprises analyzing an information of said multimedia data.

12. The method of providing access control for user terminals connected to a private network according to claim 1, wherein temporarily storing the multimedia data stream comprises storing only a part of the multimedia data stream.

13. The method of providing access control for user terminals connected to a private network according to claim 1, wherein the signature indicates an existence of restrictions on a use of the multimedia data stream.

EVIDENCE APPENDIX:

Pursuant to 37 C.F.R. § 41.37(c)(1)(ix), submitted herewith are copies of any evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 or any other evidence entered by the Examiner and relied upon by Appellants in the appeal.

Appellants are not submitting any evidence.

RELATED PROCEEDINGS APPENDIX

Submitted herewith are copies of decisions rendered by a court or the Board in any proceeding identified about in Section II pursuant to 37 C.F.R. § 41.37(c)(1)(ii).

There are no copies of decisions rendered by a court or the Board to be submitted.